UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/673,239	09/30/2003	Masashi Morioka	243403US8	5391

22850 7590 09/21/2007

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	**PAPER NUMBER**
3609	

NOTIFICATION DATE	DELIVERY MODE
09/21/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/673,239	MORIOKA ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	3609	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The language should be clear and concise and should not repeat information given in the title.

A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-8, 10-12, and 14-18 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

Claims 3 and 4 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims recite the limitation "the piece of new information". There is insufficient antecedent basis for this limitation.

Claims 3, 4, 6, 7, 9, and 18 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. "A piece of new information" is not a well defined enough term to limit the claim properly.

Claim 17 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not understood what "open means" is a reference to, nor what the term should mean in light of the application.

Claims 10 and 12 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. These claims are written in the "means-plus-function" style of language (as in 35 U.S.C. 112, sixth paragraph). However, the application not adequately set forth what is meant by the claims' language – no structure is recited in the specification.

The examiner has performed a best effort at understanding the claims, in light of the grammatical, idiomatic, antecedent, vagueness, and general linguistic errors.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 and 5-18 rejected under 35 U.S.C. 102(b) as being anticipated by CyberCash, a credit card protocol described in RFC 1898 (published by the Network Working Group on July 8, 1995, hereafter referred to as CyberCash).

As per claims 1, 15:

CyberCash teaches "several separate payment services on the Internet including credit card and electronic cash" (Cf. section 1.1, 1st paragraph). The CyberCash server receives a request from a merchant's web server ("receiving a request for usage of a service from the terminal through the information network") and selects the proper mode of operation from the received request and performs said operation, based on the "acquiring bank" ("selecting at least one situation from a plural situations of a content described in a service certificate sent from the terminal, a network environment and a system policy; and changing a service procedure and/or a message format to operate the authentication and payment system according to the selected situation") (Cf. section 1.3).

Claim 15 covers the process ("operation method") for said system, and is similarly rejected.

As per claim 5:

CyberCash is a "stateful" protocol – that is, the protocol has a "memory" or "state" and follows a pre-defined set of steps based on the data received and sent. (Compare to "stateless" which means that each transaction takes place independent of any previous ones.) At each point, the customer device ("terminal") knows where it is in the process and is waiting for a specific message to be sent. By its nature, a stateful protocol may be rolled back – if there is an error, or for logging purposes, one can follow the steps backwards to understand what has occurred ("usage history managing means configured to manage a usage history of a certificate of service...").

Furthermore, CyberCash allows the terminal to acknowledge to the server (which acknowledges to the "authentication and payment device") when it "satisfies conditions

defined in the certificate of service" (that is, it sends the CH1 message to the merchant with payment information, cf. section 1.3, 1st paragraph).

As per claim 6:

CyberCash's server receives a certificate from the merchant's server through the Internet ("a receiver configured to receive a certificate of service sent from a terminal through an information network"). It then interprets the certificate and "forwards the relevant information to the acquiring bank" (Cf. section 1.3, 2nd paragraph), using encryption (Cf. section 1.2) ("transmitter configured to transmit a request for authentication ... [with] a digital signature to an authentication and payment device through the information network, [...] wherein the request for authentication and payment is to be formed from all or a part of the certificate of service or from all or a part of the certificate of service and a piece of new information added thereto.").

As per claim 7:

Said request for authentication and payment includes the identification information of the customer (Cf. section 1.3, 1st paragraph) and relevant merchant information ("identification information including...the identification information and a piece of new information added thereto") (Cf. sections 1.3, 1st paragraph; 4.3.2, lines 14, 15; 4.4.1, lines 12-15; 4.4.2, lines 10-13). As mentioned in claim 6, digital signatures are used (Cf. section 1.2, 1st paragraph).

As per claim 8:

Said "controller configured to...simplify the processing of the request for authentication and payment" encapsulates what the CyberCash system aims to do – it enables merchants and banks to "more quickly integrate safe on-line payments into their existing service offerings" (Cf. section 1.1, 1st paragraph). This controller "configured to simplify the processing of the request for authentication and payment" and the "service providing device" are one and the same.

As per claim 9:

Said second "receiver" and second "transmitter" for sending the "generated second certificate" to the terminal are both included in CyberCash (Cf. the CH2 message in section 4.3.3).

As per claim 10:

CyberCash's server system acts as the authentication and payment device. It has "certificate of service issuing means for issuing a certificate of service to [another] device" (Cf. section 4.4.6, for the CM6 message sent from the server to a merchant),

and "processing means for processing...verification of a request for authentication and payment sent from [another] device through an information network" (Cf. section 4.4.1, for the CM1 message sent from the merchant to the server).

As per claim 11:

The server in CyberCash contains all of these features. The CM6 message (cf. section 4.4.6) contains:

- The "transaction" and "merchant-transaction" fields ("at least one piece of information of an identifier of the certificate of service"),
- the "merchant-ccid" field ("an identifier of the other device"),
- an "expiration-date" field which determines the expiration of the credit card, effectively expiring the certificate as well, since it would no longer be valid after the expiration date ("information of expiration date of the certificate of service"), and
- the "action-code" field, which (per ISO 8583) is a standard for financial transactions – the field represents what sort of action has taken place; e.g. authorization, payment, reversal ("information of constraint of service to the other device").

Additionally, because CyberCash is designed for the Internet, the IP header in the packet data containing the CM6 message would contain the server identification information e.g.: the server's IP address ("an identifier of the authentication and payment device").

As per claim 12:

CyberCash's server stores a database of transactions for auditing purposes – see section 4.4, 4th paragraph, which states that obtaining information pertinent to dispute resolution is an "auditable event" ("information storing means for storing all of a part of information which is inherently to be contained in the certificate of service as a stored information").

For dispute resolution, a merchant would need specific information about the transaction event. Referencing the transaction event using the transaction number, contained in the certificate of service, as well as "special bypass messages", would allow the merchant to obtain necessary dispute resolution information ("wherein the certificate of service contains information of a location of the stored information in the information storing means").

As per claim 13:

CyberCash's server may send a CM6 message – "given to the merchant as a receipt for a completed charge action"; see section 4.4.6 ("a transmitter configured to transmit the certificate of service to the other device in response to a request therefrom or in accordance with a predetermined condition for transmission").

As per claim 14:

CyberCash's service will respond with the CM6 message retaining some information from the CM1/CM2 message (e.g. "transaction") but updating and adding new information (e.g. "response-code" and "authorization-code"). (These messages are covered in sections 4.4.1, 4.4.2, and 4.4.6)

As per claim 16:

The CyberCash server receives a request from a merchant's web server ("receiving means of a request for use of a service") and selects the proper mode of operation from the received request and performs said operation, based on the "acquiring bank" ("analyzing means of a content of a certificate of service, a network environment and/or a system policy; and control information adaptive to at least one of plural situation of the content of the certificate of service, the network environment, and the system operation policy.") (Cf. section 1.3, 2nd paragraph).

As per claim 17:

CyberCash's server, in processing the control information, inherently must open the information in order to use it.

As per claim 18:

CyberCash's server will receive a request for service and create control information based on said request. This request (such as the CM1 message in section 4.4.1) will contain identifying information about the customer, which the server will correlate to bank information and send a request to the banking system associated with said account (cf. section 1.3, 2nd paragraph).

Claims 2-4 rejected under 35 U.S.C. 102(b) as being anticipated by US

5,870,473 (Boesch et al).

As per claim 2:

Claim 17 of Boesch reads "An electronic transfer system in a communication network for processing a transaction between a customer having a customer device, a merchant having a merchant device, and a server connected therewith, wherein the transaction has terms associated therewith and wherein the server transfers electronic funds from the customer to the merchant so that the merchant can provide a product to the customer". The server acts as the "authentication and payment system", the

customer device acts as the "terminal", and the merchant device acts as the "service providing device".

The terminal "[receives] said invoice including said portion of the terms of the transaction from said merchant device and [transmits] said portion of said customer response to the merchant device". The merchant device has received the "session" from the server, and transmits a certificate to the customer device, "including at least a portion of the terms of the transaction" ("a receiver configured to receive a first certificate of service including related information from an authentication and payment device through an information network").

The terminal will then send the "portion of [the] customer response" to the merchant device. Since this invention is designed for Internet commerce, terminal information will be sent along with the "customer response", e.g. an IP address ("transmitter configured to manipulate the first certificate of service to generate a second certificate of service including identification information of the terminal and to transmit the second certificate of service to a service providing device through the information network").

As per claim 3:

The second certificate sent to the service providing device is generated from "a part of the first certificate of service" (Cf. Boesch, claim 17).

As per claim 4:

The second certificate sent to the service providing device is generated from the "identification information" of the terminal's user (since the transmission occurs over the Internet, identification information of the terminal is sent in the IP header of the datagrams which contain the certificate) and a "piece of new information" like the "note-hash" (Cf. Figure 28A, row 5113F).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is 571-270-3462. The examiner can normally be reached on Monday-Thursday, 7:30-5, Alternate Fridays, 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Dixon can be reached on 571-272-6803. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Johns
Examiner
Art Unit 3609

ccj

THOMAS A. DIXON
SUPERVISORY PATENT EXAMINER

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :3/29/07, 3/9/06, 9/7/04, 12/17/03.